2014 International Conference on Unmanned Aircraft Systems (ICUAS)
May 27-30, 2014. Orlando, FL, USA

A Server-Based Real-Time Privacy Protection Scheme against Video Surveillance by Unmanned Aerial Systems

Yoohwan Kim, Juyeon Jo, Surendra Shrestha
Department of Computer Science
University of Nevada Las Vegas, Las Vegas, NV 89154
Email: Yoohwan.Kim@unlv.edu, Juyeon.Jo@unlv.edu, shrest16@unlv.nevada.edu

***Abstract*—Unmanned Aerial Systems (UAS) have raised a great concern on privacy recently. A practical method to protect privacy is needed for adopting UAS in civilian airspace. This paper examines the privacy policies, filtering strategies, existing techniques, then proposes a novel method based on the encrypted video stream and the cloud-based privacy servers. In this scheme, all video surveillance images are initially encrypted, then delivered to a privacy server. The privacy server decrypts the video using the shared key with the camera, and filters the image according to the privacy policy specified for the surveyed region. The sanitized video is delivered to the surveillance operator or anyone on the Internet who is authorized. In a larger system composed of multiple cameras and multiple privacy servers, the keys can be distributed using Kerberos protocol. With this method the privacy policy can be changed on demand in real-time and there is no need for a costly on-board processing unit. By utilizing the cloud-based servers, advanced image processing algorithms and new filtering algorithms can be applied immediately without upgrading the camera software. This method is cost-efficient and promotes video sharing among multiple subscribers, thus it can spur wide adoption.**

Keywords – Unmanned Aerial Systems, Video Surveillance, Privacy, Key Distribution

I. INTRODUCTION

According to the "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, 2013" [3], an Unmanned Aircraft (UA) is defined as a flying device without a pilot on-board. An Unmanned Aircraft System (UAS) is a system comprising of the UA and any other elements that are essential for the safe operation of the UA. These elements include control stations, communication data link, payloads, launch and recovery elements and the human element. There are several categories of UA based on their weight, size, speed, and payload [6, 13]. Hobby R/C airplanes are at the low end of the intelligence spectrum, while advanced UAs can fly completely autonomously.

For a long period of time, people have seen the use of UAS in the military applications. But with the recent developments in technology, government and private sectors have now discovered the use of UAS in many civilian applications such as aerial photography, fire detection and control, crime surveillance, traffic monitoring and control, etc. [1, 2, 12]. One of the most useful applications of UAS is video surveillance. UAs can be equipped with powerful cameras that are able to take high-resolution pictures and videos of the geographic regions below [8]. R/C airplanes may have raised some privacy concerns in the past, but their effect is generally limited. They fly at an altitude below 400 feet with a direct control under the operator within the Line of Sight (LOS). Thus the operators are readily identifiable and an attempt of privacy invasion can be easily spotted. UAs are much more capable than R/C airplanes, flying farther distance, possibly beyond line-of-sight (BLOS).

The surveillance image can be viewed by the surveillance operator, stored for later use, or broadcast on the Internet in real-time. This ability of the UAs has raised privacy concerns among the public [7, 21, 23]. For example, a UAS can take a video shot of people swimming in their back yard pool, as illustrated in Figure 1, or people in their bedrooms through the window.

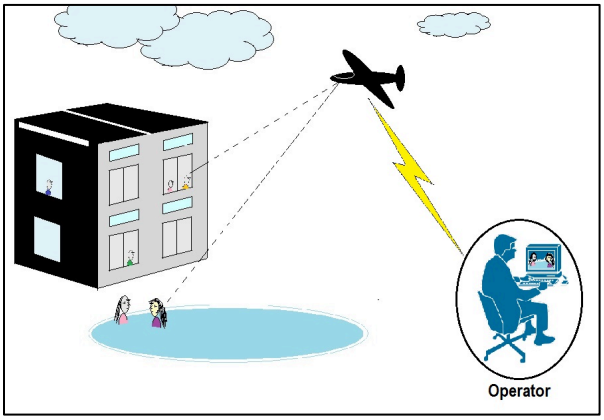

Fig. 1. UAV Snooping

In particular, a video image streamed through the Internet in real-time can become available to millions of people instantly. Once the image is published on the Internet, there is no way to turn it back. Such an inappropriate use of the UAS technology poses a serious threat to human rights for privacy and suggests a need for protection against these intrusions into privacy [20].

This paper investigates the privacy problems related with UAS, current efforts to protect privacy against UAS, and proposes a scheme that can be employed widely in a cost-efficient way. The rest of the paper is organized as follows. Section II introduces the concerns caused by UAS. Section III discusses possible technical solutions to protect privacy. Section IV describes the proposed privacy protection

scheme. Sections V and VI discuss some implementation issues. Section VII shows a generalized architecture where multiple privacy servers and UASs are involved. Section VIII summarized the advantages of the proposed architecture compared with other schemes. Section IX addresses some challenges such as the need for Internet connection, attacks from the Internet, and communication delay. We then conclude the paper in Section X.

II. PRIVACY CONCERNS

Privacy is "*the state or condition of being free from being observed or disturbed by other people*" [15]. Privacy is a relatively subjective concept, and different people react differently. It also varies by society or by era or generation. A privacy-invading incident may be perfectly acceptable for some, but may be totally unacceptable to others. This complexity requires a method to apply different types of privacy protection schemes than a single uniform strategy.

In the recent years, the number of UAS being operated has risen greatly and is expected to rise further in the coming years. With the high quality video surveillance cameras being used in the UAS to monitor the activities happening in the ground, the chance of inadvertent privacy invasion is increasing. Night operation poses a greater threat, as it is nearly impossible to locate a UAS at night due to its low visibility and silent operation, while it is now possible to view the night images in high definition with full color instead of gray IR video [16].

However, video surveillance is not new. We are living in a world where we are constantly being watched [18]. There are CCTV cameras nearly in every public places, road, campus, bar, bus station, office buildings, etc. This prevalence of CCTV image has actually helped to track down the suspects in the Boston Marathon Bombing attack in 2013 [9]. Google Street View and numerous satellite images in search engines are available to public. However, all those images are taken in public places and the chance of privacy violation is low. In case of Google Street View, the images are not available in real-time and it is carefully censored to blur the car plate numbers or people's faces. In case of those commercial entities, tracking the company violating the privacy law is trivial. However, in case of UAS, the surveillance operator is not easily traceable. The video can go viral instantly on the Internet as it happens, and worse, we cannot identify who is responsible for that. This is a serious threat to general public, and a number of states have already created anti-UAS law reflecting the fear against the privacy invasion by UAS [4, 5, 22]. Without answering these concerns in a trusted manner, both from policy/legal and technical side, a wide adoption of UAS for civilian usage could be hampered.

III. RELATED WORK

Although the privacy invasion from UASs is a serious threat, there has been very few published works on this topic. This section discusses possible solutions that are available or being discussed informally within the research community.

A. Increasing visibility

One of the problems with UAS-based surveillance is that the people who are surveyed are generally unaware of it because of UAs' low visibility. They are small and they generate very low noise [12]. By mandating a flashing light and sound warning (*e.g.,* beeping), people can become aware of them. While taking video, additional warning may be given, like blinking red light similar to camcorders'.

B. Geo-Fencing

Geo-fencing is a feature that uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries [10, 11]. A geo-fence creates a virtual barrier so that a moving object cannot enter or exit cross the virtual wall. A geo-fence can be a predefined set of boundaries, like school attendance zones or neighborhood boundaries, or it could be dynamically generated. The geo-fencing concept is not new in airspace control. Airplanes may not enter a restricted airspace. The geo-fencing concept is now being applied to UAS in fine-grain [19]. However, the concept of geo-fencing may be too rigid for an efficient operation of UAS. It may require an unnecessary detour. Not all privacy-protected airspace is a restricted airspace, so they should be still able to fly in there. If a surveillance target region is surrounded by geo-fence, the region will not be accessible even if it allows video surveillance. Therefore a softer alternative is desirable.

C. Blanking Technique

The blanking technique erases a certain portion of the video if the portion is privacy-protected. The on-board camera should not be allowed to take the video of areas where people have a higher expectation of privacy such as restrooms [24]. The camera and the on-board processing system determine whether the region is protected, and, if protected, blanks out the section of the video before transmitting the video to the ground station (Figure 2). So an accidental release of the privacy-protected video is prevented as the decision is made by the on-board processing unit before the human operator can view it. This method requires an on-board processor with a pre-loaded privacy map of the surveyed region. Although blanking technique is currently the most intuitive and viable solution, there are some shortcomings.

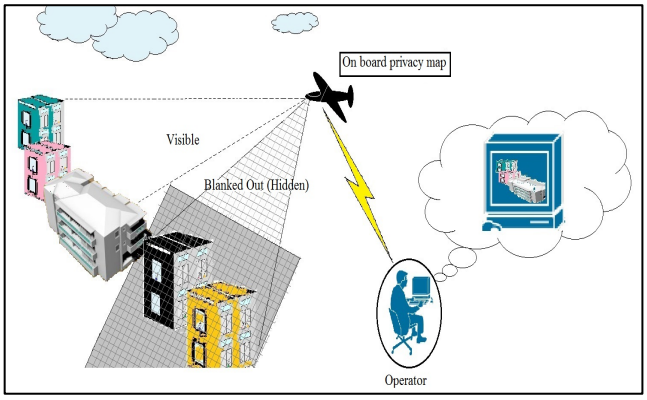

Fig. 2. Blanking Technique

1) Need for on-board map and processing system

This technique requires specialized maps and high-performance on-board computing systems. While this is not impossible, there are some undesirable consequences. The need for larger memory and high-performance computing system increases the cost, which directly impacts the affordability of the system and slows the adoption rate. Furthermore, those added equipment consumes more power and reduce the battery life. The increased weight also reduces the speed, range, and flight duration of the UA.

2) Static privacy map

The on-board privacy map is static and not updated in real-time. It is a snapshot of the privacy requirements, and the map is frozen until next update. If a person spots a UAS flying and taking a video over his house, there is no way to stop it because on-demand request in real-time is not possible. Secondly, updating the map and on-board software is the responsibility of the UAS operator. But with a large UAS fleet, it takes significant time and effort to update them in all UAs, and thus it may be neglected.

3) Non-compliant usage

Use of the blanking algorithm is purely voluntary. The operators can turn off the algorithm and take the video freely at the private regions. It is difficult to check whether the algorithm is being used as required or audit it afterwards. Even if an audit can be done afterwards, the video may have been already released to the public by the time it is audited. The lack of audit feature hurts not only the victims but also the surveillance operator. If there is any criminal charge or lawsuit against the operator, the operator may not be able to prove the algorithm was properly used.

IV. PROPOSED SCHEME

We propose a lightweight real-time privacy protection scheme with multiple levels of privacy. This scheme uses a cryptographic process to encrypt the video at the camera and decrypt it at a trusted 3rd party server. Since the privacy filtering operation is done at a powerful cloud-based server on the ground, the UA doesn't need to carry sophisticated computing equipment as in blanking technique. The privacy detection algorithm, privacy map, filtering software can be upgraded separately from the camera system. Thus the same camera can be used for a longer period without upgrading.

A. Architecture

The architecture is shown in Figure 11 in the Appendix. The video taken by a UA is encrypted always. The surveillance operator's equipment receives it, but it cannot decrypt the video because it does not have the decryption key. It only relays the encrypted video to a privacy server.

The encrypted data is unencrypted at a cloud-based privacy server, and analyzed based on the most up-to-date privacy policy. After the filtering operation, the sanitized video is sent to the surveillance operator. The privacy policy at the privacy server can be modified any time on demand. Any privacy requirements and violation can be monitored and enforced in real-time at the server.

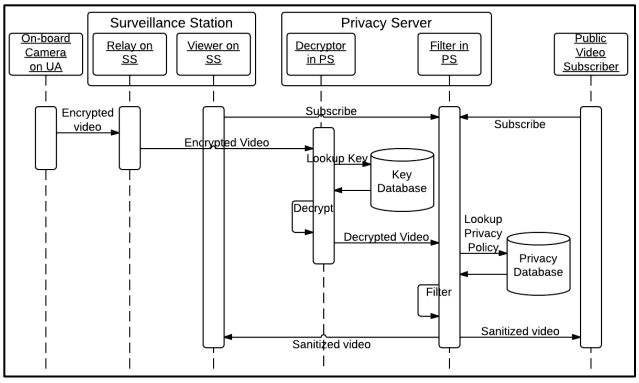

Fig. 3. Interaction Among Participants

B. Operating Procedure

The operating sequence is shown in Figure 3.

1) Camera certification and key assignment

The camera is equipped with a shared symmetric key with the privacy server. It is suggested that the key should be stored in a Trusted Platform Module (TPM) to avoid key theft. The IP address of the privacy server(s) is pre-configured in the camera.

2) Camera owner registers the privacy service subscription with the PS.

After purchasing the camera, the owner creates an account and registered the camera ID.

3) Key confirmation

Upon powering up, the camera looks for the privacy server and they confirm proper communication. The camera may operate in non-encryption mode with lowest resolution before the connection with the server is made.

4) Privacy filtering

When the encrypted video image comes to the privacy server, the server decrypts it and looks up the privacy policy for the region. As well as static filtering based on the location, a dynamic filtering can be applied with image-processing algorithms to filter out any inappropriate video.

5) Sanitized video delivery

The resulting sanitized video is delivered to the surveillance operator or anyone with an authorization.

C. Cryptographic Scheme

The 3-tier model (camera, surveillance station, privacy server) may look similar to 802.11i protocol [17] where the Authenticator (access point) passes the message from the Supplicant (wireless client) to the Authentication server (RADIUS). However, there is a fundamental difference. The video stream from the UA to the privacy server is a broadcast in essence. The privacy server doesn't need to authenticate any camera with a handshake sequence. The encrypted channel is already established with a pre-shared key. The camera doesn't need to authenticate the privacy server, either. If the camera contacts a wrong privacy server, the data cannot be decrypted and privacy is not

compromised. To explain the encryption process, we denote the entities as following.

- Surveillance Station = SS
- Privacy Server = PS

There is no encryption between any entities at the data link layer.

- UA → SS: Proprietary wireless channel (No encryption)
- SS → PS: Public Internet (No encryption)

The video stream is packetized and encrypted in the following format.

- V = [video data, sequence number, hash]

The encrypted video data is delivered from UA to the PS via SS. The SS packages it within an IP packet, and sends it to the PS. SS is not part of the cryptographic process. It simply relays the encrypted video stream to PS.

K is the shared key between UA and PS.

- UA → SS: {Camera ID | E (V, K)}
- SS → PS: {Camera ID | E (V, K)}
- PS: D (E (V, K)) = V,
  SV = Filter (V)
- PS → SS: {SV}

For the encryption, we propose to use a simple block cipher mode with AES [17]. Currently AES is considered the strongest encryption algorithm. To use AES for stream cipher, we employ Counter (CTR) mode for its efficiency. Counter mode works as illustrated in Figure 4 [17].

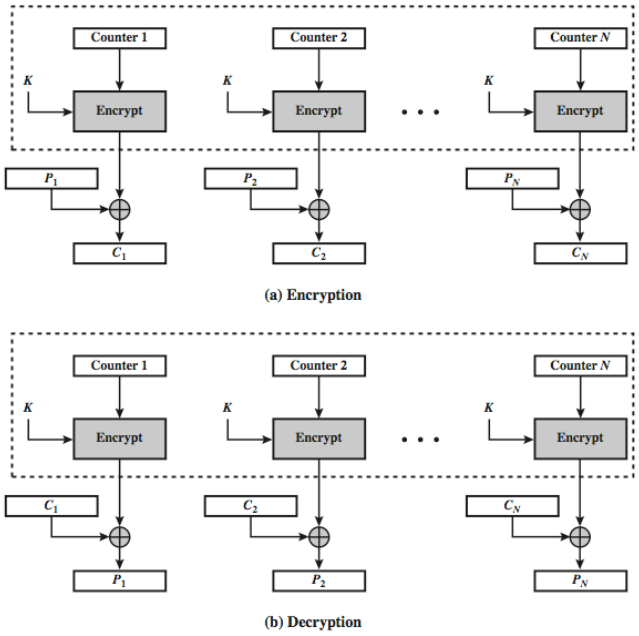

Fig. 4. Block Cipher with CTR Mode [17]

Unlike other block cipher modes, the goal of the Counter mode is generating a random key stream to be used for stream cipher. All plaintext inputs are XORed with this key stream to produce a ciphertext. During the decryption process, the same key stream is created and then XORed with the ciphertext to produce the plaintext.

The size of the counter value must be sufficiently large to avoid recycling because a reused counter value could be used for a cryptanalysis attack. A 48-bit value may be acceptable to avoid recycling. Given the encryption block size of 128-bit (2^7 bits) and the bandwidth of a high definition video stream of, for example, 4 Mbps (2^{22} bits/sec), the video will generate 2^{15} blocks per second. In other words, the counter value will repeat after 2^{33} seconds (= 2^{48} /2^{15}), which will take more than 1,000 years even if the video is continuously transmitted without stopping.

V. TYPES OF DATA AND MULTI-LEVEL PRIVACY

UAS collects different types of data from various locations. For each type of data, there may be different requirements for privacy protection. For simplicity we limit the type of data to video data. The video data input can be categorized into different levels and relevant privacy schemes may be applied. With this scheme, the public can fine-tune their privacy preference.

A. Navigation-Critical Data

First we categorize the data into navigation-critical data and navigation-neutral data. We should mention that, navigation does not rely only on camera. In many cases, camera input is not used at all for navigation [14]. The Sense-and-Avoid (SAA) functions do not use camera. The See-and-Avoid function may use a camera, but it does not rely on a high-resolution camera. For collision avoidance and navigation, only the general shape of the object, color, or brightness levels are sufficient, thus low-resolution cameras may be sufficient.

B. Meta Data

Complete erasure of the video may be too limiting for the surveillance operation. Some level of summary data may be released to the surveillance operator. For example, the privacy-protected region may display a text output such as, "pool", "bedroom", "person sleeping on the grass", "person smoking", or "restroom". High-quality meta data or summary data after filtering may improve the utility of the surveillance operation. Navigation-critical video data can be also transformed into a non-privacy invading forms, such as size, location, mobility, or meta data forms.

C. Levels of Privacy

The privacy requirements for video surveillance can be categorized as following. Figure 7 illustrates the varying levels of video quality. The default mode can be set to 5).

1) *No video or meta data allowed*
2) *No video allowed*
3) *Mosaic image allowed*
4) *Low-resolution video allowed*
5) *High-definition video allowed*

In some cases, people may feel annoyed when a UAS flies nearby in a low altitude. They should be able to set the minimum distance from their location. For example,

1. More than 1000 feet
2. More than 500 feet
3. More than 100 feet
4. More than 50 feet
5. Landing allowed

The above rules can be applied only during a certain time period. For example,

1. Applied at all times
2. Applied only at day time
3. Applied only at night time
4. Applied only in specific time or day

Outside of this period, it will fall back to the default privacy level. Table 1 shows a sample privacy policy database incorporating the multi-level privacy requirements.

VI. PRIVACY PROTECTION FILTERING

Within the privacy server, the filtering module performs a filtering operation according to the privacy database. The result of filtering may be blanking out the whole scene, blurring the scene, with mosaic images, or scaling down the resolution. This video transformation could be applied to the entire video image or a small section of the video. There are three ways to apply the privacy policy as follows.

A. Static Filtering

The privacy server keeps the privacy protection levels based on the location and the municipal regulations. The UAS sends the information on camera's view such as,

- Current location of UAS
- Camera direction
- Distance to the object

The UAS may also report the flight direction, so that the privacy server can predict the oncoming privacy level change, and warn the UAS to avoid the region. Privacy server determines the camera's field of view and the resolution of the pictured object. The resolution of the image at the target object should be determined in consideration of the distance. Figure 5 shows two cases where the video resolution can be equivalent. It looks up the privacy policy table, and applies a necessary policy.

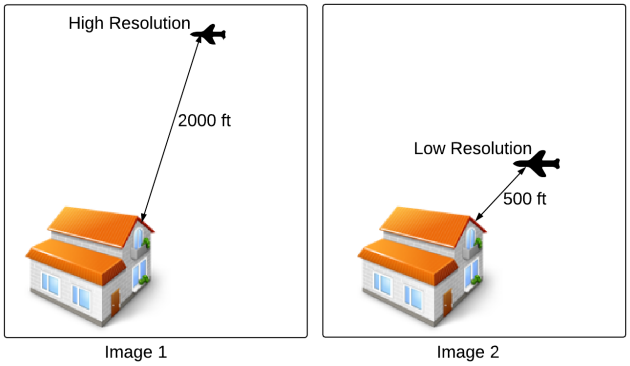

Fig. 5. Equivalent Video Quality

B. On-Demand Filtering

When a UAS is spotted taking video, a person concerned with his or her privacy may request not to take the picture, or change the privacy level. Figure 6 shows a mock up mobile web page to request privacy protection. A victim can type the address of the desired location for privacy protection. This information is delivered to the privacy server, and immediately become effective. Furthermore, if the victim wants to protect the location around him continuously while he is moving, he can choose to transmit his GPS coordinate continuously.

Fig. 6. Privacy Protection Request in Real-Time

Fig. 7. Varying Levels of Privacy

TABLE I. SAMPLE PRIVACY POLICY DATABASE

Latitude	Longitude	Address	Privacy level	Distance	Time period	Target type
X1 to X2	Y1 to Y2	234 Main St, Town, State	Low res video	> 1000 feet	only at night time	Residence
X3 to X4	Y3 to Y4	987 Pool Ave, Town, State	Meta data	> 500 feet	only at day time	Community pool
X5 to X6	Y5 to Y6	543 Some Rd, Town, State	No video	> 100 feet	at all times	School play ground
X7 to X8	Y7 to Y8	775 What Ct, Town, State	Low res video	Landing allowed	only at day time	Park

C. *Processed Filtering*

The privacy server employs advanced image processing algorithm and actively processes the image to search a scene that violates privacy even if it is not specified in the privacy policy table. When it detects one, it takes a relevant action such as blurring the face or replacing it with meta data.

VII. GENERALIZED ARCHITECTURE

The simple camera-to-privacy server model needs to be extended to cover a large number of UAS and multiple privacy servers. A UAS should be able to connect to any privacy server available. Figure 8 describes the generalized architecture.

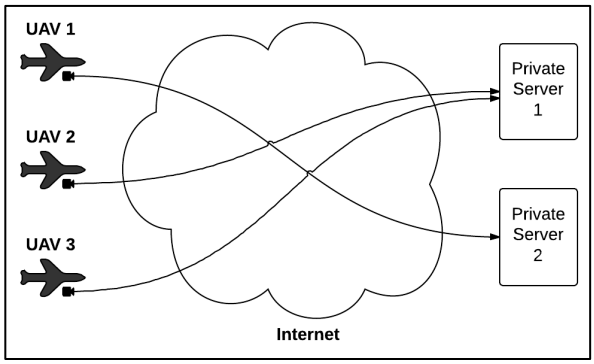

Fig. 8. Generalized Architecture with Multiple Cameras and Servers

A. *Encryption Key Distribution*

Before starting the video surveillance operation, the cameras and the privacy servers need to share a key. It is impractical for all the servers to keep the key information individually for thousands or cameras. We propose to use Kerberos model, a key distribution protocol that are commonly used in network-based key distribution such as Microsoft Active Directory [17]. The Kerberos Key Distribution Server is composed of two servers. Initially all cameras register their key at Authentication server (AS), and Privacy Servers register their key at the Ticket Granting Server (TGS) as shown in Figure 9. After the initialization, the registered keys are never used for data encryption, but used only for distributing the session keys.

Figure 10 illustrates the process of key distribution. At the beginning of the surveillance operation, the camera contacts the AS. In steps (1) and (2), the camera receives Ticket Granting Ticket (TGT) containing a long-term session key to access to Ticket Granting Server (TGS). By presenting the TGT to TGS (3), the camera obtains a ticket (4) that contains a short-term key to access the desired privacy server. If the particular privacy server is busy, the camera can ask for a new Ticket for a different server.

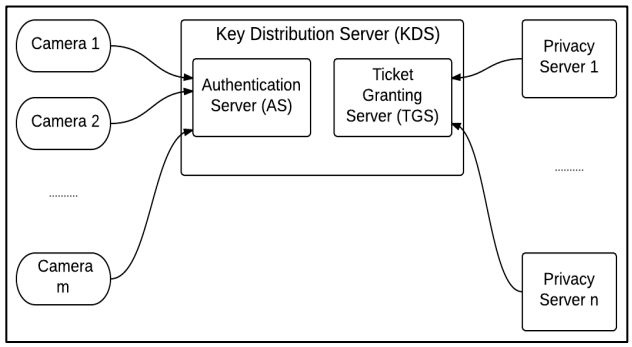

Fig. 9. Key Registration at Kerberos

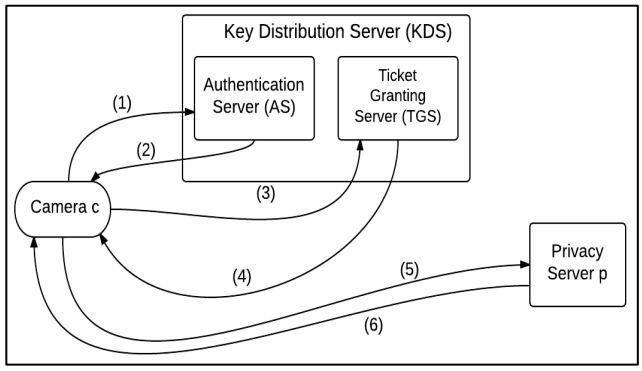

Fig. 10. Key Distribution in the Field

B. *Video Subscription Management*

Independently from the encryption/decryption operation, it is necessary to decide who gets the sanitized video stream. The owner of the camera can manage the access rights. At the time of purchasing, he or she establishes the ownership and creates a management account. From this account, he or she can allow the IP address or particular users to get the video image. The owner's surveillance station shall be obviously the first allowed machine, but he or she can also allow other people to access the video.

VIII. ADVANTAGES

This proposed scheme has a number of advantages over conventional blanking technique.

A. *Flexible Privacy Policy*

The privacy policy for the proposed scheme is applied on the ground, unlike the blanking technique. This feature gives an advantage in that the privacy policy can be modified in real-time when needed. Based on the privacy policy, multiple levels of privacy can be designed depending on the sensitivity level of the surveyed region.

B. Separation of Camera from Image Processing

The video image processing is done at a cloud-based privacy server. So the owner of the camera doesn't need to worry about upgrading the camera's software. Advanced image processing algorithms can be immediately applied without a camera software upgrade. Therefore, a relatively low cost camera can be used for a longer period. Also, by sharing the common privacy server among multiple camera owners, the cost for using the privacy server can become lower. This lowers the price of the system, which may increase the adoption rate.

C. Legal Protection

If a surveillance operator uses an approved camera, he or she is better protected from a legal problem because the compliance to the privacy policy is automatically ensured. Operators may prefer using a compliant camera to their own non-compliant camera. For government entities, this could be a great relief because they don't become liable for privacy invasion. It is similar to the car-mounted video camera in police cars where policemen can prove that they didn't do anything illegal while investigating an incident. The original unfiltered video can be stored and fully decrypted later with a proper authorization if there is a need for an incident investigation.

D. Supporting Forensic Investigation for Privacy Violation

Since the video stream is monitored and archived at the privacy server, real-time compliance checking or auditing can be done easily. Upon any violation, the law enforcement can investigate the incident with the stored data. The logging data types, logging process, and cryptographic verification process will need to be developed.

E. Availability of the Video to a Larger Audience

With the cloud-based privacy server model, video sharing becomes a built-in feature. It allows real-time video sharing over the Internet with whoever is authorized to watch. For example, in a kids' soccer game, one person may fly a UA to take a video and the video is fed to a privacy server. The operator gives the account information to the parents who are watching the game, and they all can watch the aerial footage without a hassle. Any unsuitable scene for young children or private scene can be filtered out in real-time, so everyone can enjoy a family-friendly video. This video can be also saved at the privacy server and watched later.

IX. DISCUSSIONS

A. Need for High-Bandwidth Internet Connectivity

The greatest disadvantage with the proposed scheme is the need for constant Internet connection. With the prevalence of the wireless Internet coverage, this shouldn't be an issue normally. However, in remote places where no wireless Internet is available, we need to have a backup method. A mobile privacy server can take a snapshot of the current privacy policy in the surveyed region, and sanitize the video on the spot. This may work because there is probably less privacy concern in remote places and the privacy policy is less frequently updated.

The Internet connection to the privacy server has to provide a sufficiently high bandwidth for the video transmission. In reality, this bandwidth does not need to be very high because the image from an on-board camera is converted to a low-resolution below VGA (640 x 480) due to the limited bandwidth of the wireless channel. The original high-resolution image (1920 x 1080) is recorded in the on-board storage and retrieved upon landing. The VGA video at 30 frames per second requires 1 to 1.5 Mbps of bandwidth, which is not challenging in today's Internet.

B. Communication Delay

Another issue is the perceivable delay in video due to the round-trip of the video between the surveillance station and the privacy server. Although this delay is small, most likely less than a second, it may still annoy some UAS operators. We solve it with a novel method of real-time key stream delivery. If real-time video decryption is necessary, the privacy server delivers the key stream to the surveillance station. Then the operator can decrypt the video image received from the camera in real-time, and watches the video without any delay. When the key stream stops, the decryption stops, too. Meanwhile, the privacy server continues to analyze the video as before. If the pictured region is a privacy-protected region, the privacy server stops sending the key stream to prevent the video from being decrypted or send a control data to lower the resolution. When the camera takes a video from a non-protected region, the privacy server resumes sending the key stream.

If high definition video is stored in an on-board storage device, *e.g.,* SD memory card, it will be stored in an encrypted format. When the UAS operator retrieves the memory card and inserts it into the surveillance station equipment, the key stream and control data are delivered from the privacy server for permanent off-line viewing.

C. False Privacy Data Injection

If a malicious user submits the privacy protection requests for every location, the UAS system cannot take any useful video. Therefore it is important to reject bad requests to keep the privacy server useful. To minimize such a malicious use, we may ask the users to submit identity information, *e.g.,* credit card number, and limit the number of requests per day, or limit the valid period of the request.

D. Denial of Service attack

A hostile entity may flood the privacy server with a large amount of traffic to create a Denial-of-Service condition. [17]. Any server on the Internet is vulnerable to this attack, and our privacy server is no exception. Many techniques have been developed to thwart them, and readers are encouraged to follow the recent develop on this topic.

X. CONCLUSIONS

In this paper, we have reviewed privacy policies, protection strategies, and technical solution for UAS-based video surveillance. Blanking technique with an on-board processing unit is currently the most intuitive solution, but the high cost and the need for upgrading the privacy map

and software could slow its adoption. We proposed an alternative privacy-protection method with a lower cost of implementation. In this scheme, all video surveillance images are initially encrypted, then delivered to a cloud-based privacy server. The privacy server decrypts the video using a shared key with the camera, and filters the image according to the privacy policy for the surveyed region. We also studied multiple privacy levels and different filtering strategies. In a larger system composed of multiple cameras and multiple privacy servers, the key can be distributed using the Kerberos protocol. This method has several advantages including lower system cost, applicability of advanced image processing algorithms, legal protection for the UAS operators, and real-time streaming video availability to general public on the Internet, all of which may promote a wide adoption.

REFERENCES

[1] A. R. Girard, A. S. Howell and J. K. Hedrick, "Border Patrol and Surveillance Missions using Multiple Unmanned Air Vehicles," in 43rd IEEE Conference on Decision and Control, pp. 620-625, 2004.

[2] Congress of the United States, Congressional Budget Office, "Policy Options for Unmanned Aircraft Systems," June 2011.

[3] U.S. Department of Transportation Federal Aviation Administration, "Integration of civil unmanned aircraft systems (UAS) in the National airspace system (NAS) roadmap," 2013.

[4] J. Stanley and C. Crump, "Protecting privacy from aerial surveillance: Recommendations for Government use of drone aircraft," American Civil Liberties Union (ACLU), Dec. 2011.

[5] J. Villasenior, "Will Drones Outflank the Fourth Amendment?" Forbes Magazine, Opinion, Sept. 20, 2012.

[6] Federal Aviation Administration, "Fact Sheet Unmanned Aircraft Systems (UAS)," July 2011.

[7] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," pp. 1-30, 2012.

[8] K. Dalamagkidis, K.P. Valavanis, L.A. Piegl, "Current Status and Future Perspectives for Unmanned Aircraft System Operations in the US," Journal of Intelligent and Robotic Systems, vol. 52, pp. 313-329, 2008.

[9] "CCTV: suspects in Boston Marathon bombings". Internet: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10004981/CCTV-suspects-in-Boston-Marathon-bombings.html, Apr. 18, 2013 [Accesed on Feb 16, 2014]

[10] H. Rahimi, A. N. Zincir-Heywood and B. Gadher, "Indoor geo-fencing and access control for wireless networks", 2013 IEEE Symp on Computational Intelligence in Cyber Security (CICS), 2013.

[11] F. Reclus and K. Drouard, "Geofencing for fleet and freight management," in 9th International Conference on Intelligent Transport Systems Telecommunications (ITST), pp. 353-356, 2009.

[12] R.K. Barnhart, S.B. Hottman, D.M. Marshall and E. Shappee, "Introduction to Unmanned Aircraft Systems," CRC Press, 2012.

[13] K. Dalamagkidis, K.P. Valavanis, L.A. Piegl, "On Integrating Unmanned Aircraft Systems into the National Airspace System," Springer, 2009.

[14] P. Angelov, "Sense and Avoid in UAS," Wiley, 2012.

[15] Google Dictionary. Internet: https://www.google.com/search?q=define+privacy&oq=define+privacy&aqs=chrome..69i57j0l2j69i60j0l2.3091j0j7&sourceid=chrome&espv=210&es_sm=122&ie=UTF-8, [Accesed on Feb. 17, 2014].

[16] Axis Communications. Internet: http://www.axis.com, [Accesed on Feb 17, 2014].

[17] W. Stallings, "Network Security Essentials: Applications and Standards," Prentice Hall, 2011.

[18] "CCTV Security Systems Explained." Internet: http://www.brickhousesecurity.com/category/video+surveillance+security+cameras/about+cctv+cameras.do, [Accesed on Feb 17, 2014].

[19] A.M. Antonopoulos, "Geo-Fencing for ArduCopter - Keep your copter "fenced in"." Internet: http://diydrones.com/profiles/blogs/geo-fencing-for-arducopter-keep-your-copter-fenced-in, Apr. 28, 2012 [Accesed on Feb 17, 2014].

[20] "Domestic Unmanned Aerial Vehicles (UAVs) and Drones". Internet: http://epic.org/privacy/drones, [Accesed on Feb. 16, 2014].

[21] Dee Ann Divis, "UAV Operations in National Air Space Advance as Privacy Fight Heats Up". Internet: http://www.insidegnss.com/node/3687, [Accesed on Feb. 16, 2014].

[22] Chip Somodevilla, "Lawmakers voice concerns on drone privacy questions". Internet: http://nbcpolitics.nbcnews.com/_news/2013/03/20/17389193-lawmakers-voice-concerns-on-drone-privacy-questions?lite, Mar. 20, 2013 [Accesed on Feb. 16, 2014].

[23] "Concerns over UAV Privacy Issues Continue". Internet: http://www.rotor.com/Publications/RotorNews/tabid/843/articleType/ArticleView/articleId/2281/Concerns-over-UAV-Privacy-Issues-Continue.aspx, Apr. 4, 2013 [Accesed on Feb 16, 2014].

[24] Ann Cavoukian, "Privacy and Drones: Unmanned Aerial Vehicles", http://www.ipc.on.ca/images/Resources/pbd-drones.pdf, Information & Privacy Commissioner, Ontario, Canada, Aug, 2012, pp. 18-19, [Accessed on May 9, 2014]

APPENDIX

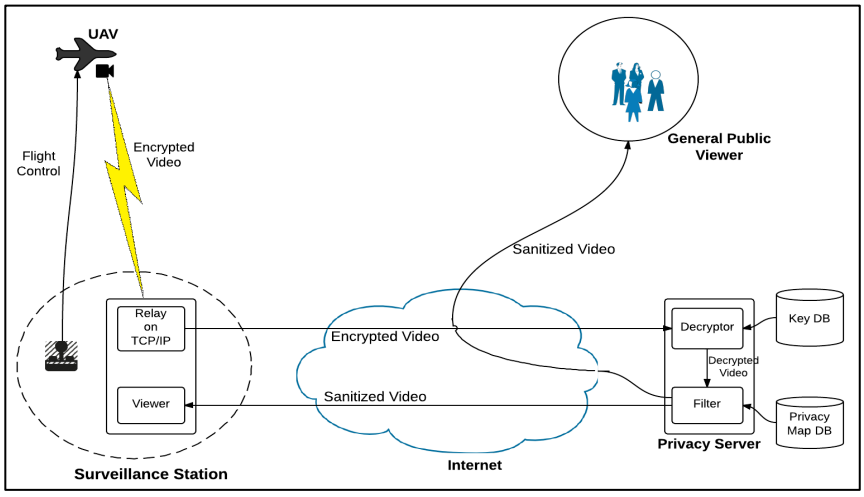

Fig. 11. UAS Architecture